IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

GENEVIEVE TAMBRONI, JOHN LATTIMORE, as parent for minor children S.L. and V.L., ELLA WILLIAMS, JAMES BEACH, CAITLIN McDANIEL, CLAUDINE KING and IAN CURRO, *individually and on behalf of all others similarly situated*, Plaintiffs, v. WELLNOW URGENT CARE, P.C., ADMI CORP d/b/a/ TAG – THE ASPEN GROUP, and PHYSICIANS IMMEDIATE CARE LLC, Defendants.	Case No. 1:24-cv-01595 [JURY TRIAL DEMANDED] This Document Relates To: All Actions

CONSOLIDATED CLASS ACTION COMPLAINT

Representative Plaintiffs Genevieve Tambroni, John Lattimore, (as parent for minor children S.L. and V.L), Ella Williams, James Beach, Caitlin McDaniel, Claudine King, and Ian Curro (collectively "Representative Plaintiffs") bring this Consolidated Class Action Complaint against Defendant Aspen Dental Management, Inc. or its parent company, WellNow Urgent Care, P.C., ADMI Corp. d/b/a TAG - The Aspen Group and Physicians Immediate Care LLC, (collectively, "Aspen Dental" or "Defendants") for their failure to properly secure and safeguard Representative Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendants' information network, including, without limitation, full names, Social Security numbers, driver's license/state ID information, health information, health insurance information, dates of birth, financial account information, biometric

data, and other sensitive information (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

INTRODUCTION

1. With this action, Representative Plaintiffs seek to hold Defendants responsible for the harms they caused and will continue to cause Representative Plaintiffs and, at least, 515,000 [3] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants on April 25, 2023, by which cybercriminals infiltrated Defendants' inadequately protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected (the "Data Breach").

2. Representative Plaintiffs further seek to hold Defendants responsible for not ensuring the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[3] https://www.classaction.org/data-breach-lawsuits/wellnow-aspen-dental-march-2024#:~:text=TAG%20Urgent%20Care%20Support%20Services,attack%20on%20April%2025%2C%202023 (last visited May 30, 2024).

A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

3. While Defendants claim the Data Breach occurred on April 25, 2023, Defendants did not begin informing victims of the Data Breach until nearly ten months later and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendants informing them of it. The Notices received by Representative Plaintiffs were dated February 22, 2024.

4. Defendants acquired, collected and stored Representative Plaintiffs' and Class Members' PHI/PII. Therefore, at all relevant times, Defendants knew or should have known that Representative Plaintiffs and Class Members would use Defendants' services to store and/or share sensitive data, including highly confidential PHI/PII.

5. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and insurers, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendants' maintenance of Representative Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

6. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

7. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' PHI/PII, Defendants assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiffs do not bring claims in this action for direct violations of HIPAA, but charge Defendants with various legal violations merely predicated upon the duties set forth in HIPAA.

8. Defendants disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

9. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class and at least one other Class Member is a citizen of a state different from Defendants.

10. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper under 28 U.S.C. § 1367.

11. Defendants are headquartered and routinely conduct business in the state where this district is located, have sufficient minimum contacts in this state and have intentionally availed themselves of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this state.

12. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this judicial district and Defendants do business in this judicial district.

THE REPRESENTATIVE PLAINTIFFS

Plaintiff Genevieve Tambroni

13. Plaintiff Genevieve Tambroni is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New York and is a victim of the Data Breach.

14. Defendants received highly sensitive PHI/PII from Plaintiff in connection with the services she received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

15. At all times herein relevant, Plaintiff is and was a member of the Class.

16. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

17. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

18. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach."

19. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

20. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

21. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety over increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

22. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

23. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff John Lattimore

24. Plaintiff John Lattimore is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New York. Plaintiff Lattimore acts on behalf of his minor children, S.L. and V.L., who are victims of the Data Breach.

25. Defendants received highly sensitive PHI/PII from Plaintiff in connection with the services he received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

26. At all times herein relevant, Plaintiff is and was a member of the Class.

27. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

28. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Representative Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

29. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

30. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

31. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

32. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety over increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

33. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

34. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Ella Williams

35. Plaintiff Ella Williams is an adult individual, and at all relevant times herein, was a resident and citizen of the State of Washington and is a victim of the Data Breach.

36. Defendants, specifically Aspen Dental, received highly sensitive PHI/PII from Plaintiff in connection with the services she received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

37. At all times herein relevant, Plaintiff is and was a member of the Class.

38. As required in order to obtain services from Defendants, Representative Plaintiff provided Defendants with highly sensitive PHI/PII.

39. Representative Plaintiff PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

40. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

41. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

42. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

43. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

44. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

45. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff James Beach

46. Plaintiff James Beach is an adult individual, and at all relevant times herein, was a resident and citizen of the State of Pennsylvania and is a victim of the Data Breach.

47. Defendants, specifically Aspen Dental, received highly sensitive PHI/PII from Plaintiff in connection with the services he received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

48. At all times herein relevant, Plaintiff is and was a member the Class.

49. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

50. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

51. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

52. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

53. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

54. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

55. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

56. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Caitlin McDaniel

57. Plaintiff Caitlin McDaniel is an adult individual, and at all relevant times herein, was a resident and citizen of the State of California and is a victim of the Data Breach.

58. Defendants, specifically Aspen Dental, received highly sensitive PHI/PII from Plaintiff in connection with the services she received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

59. At all times herein relevant, Plaintiff is and was a member of the Class.

60. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

61. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

62. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

63. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

64. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

65. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

66. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

67. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Claudine King

68. Plaintiff Claudine King is an adult individual and, at all relevant times herein, a resident and citizen of the State of Illinois and is a victim of the Data Breach.

69. Defendants received highly sensitive PHI/PII from Plaintiff in connection with the services she received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

70. At all times herein relevant, Plaintiff is and was a member of the Class.

71. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

72. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

73. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

74. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

75. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

76. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

77. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

78. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Ian Curro

79. Plaintiff Ian Curro is an adult individual and, at all relevant times herein, a resident and citizen of the State of New York and is a victim of the Data Breach.

80. Defendants received highly sensitive PHI/PII from Plaintiff in connection with the services he received. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

81. At all times herein relevant, Plaintiff is and was a member of the Class.

82. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive PHI/PII.

83. Plaintiff's PHI/PII was exposed in the Data Breach because Defendants stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

84. Plaintiff received a letter from Defendants, dated February 22, 2024, stating Plaintiff's PHI/PII was involved in the Data Breach.

85. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

86. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

87. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

88. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII, in combination with Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

89. Plaintiff has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

DEFENDANTS

90. Defendant Aspen Dental Management, Inc. is an American dental support organization incorporated in Delaware with a principal place of business located at 806 W. Fulton Market in Chicago, Illinois 60607. Defendant Aspen Dental Management, Inc. is a dental care provider that has a network of more than 1,000 locations nationwide and "is the largest group of branded dental offices in the world."[4]

91. Defendant ADMI Corp. d/b/a TAG – Aspen Dental is a Delaware corporation with a principal place of business located at 800 Fulton Market, Chicago, Illinois 60607. TAG is the parent company for Defendant WellNow Urgent Care, P.C.

[4] *See About Aspen Dental*, https://aspendental.mediaroom.com/2024-02-06-Aspen-Dentals-You-1st-Campaign-Embraces-25-Years-of-Perfecting-a-Proven-Model-and-Investing-Back-into-Clinician-Development (last visited May 30, 2024).

92. Defendant WellNow Urgent Care, P.C. is a New York corporation with a principal place of business located at 311 N Green St., Fl 17, Chicago, Illinois 60607. Defendant WellNow Urgent Care, P.C. operates various urgent care facilities,[5] acquired Defendant Physicians Immediate Care in 2022 and is part of TAG - The Aspen Group.[6]

93. Defendant Physicians Immediate Care LLC is a Delaware corporation with a principal place of business located at 1700 W. Higgins Rd., Ste. 600, Des Plaines, Illinois 60018. Defendant Physicians Immediate Care LLC was acquired by Defendant WellNow Urgent Care, P.C. in 2022.[7]

94. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

95. In the course of the Data Breach, one or more unauthorized third parties accessed Representative Plaintiffs and Class Members' sensitive data, including, but not limited to, full names, Social Security numbers, driver's license/state ID information, health information, health

[5] "WellNow Urgent Care," *WellNow Urgent Care*, https://www.wellnow.com/ (last accessed May 30, 2024).

[6] "WellNow Urgent Care Acquires Physicians Immediate Care," *Wellnow Urgent Care,* https://www.wellnow.com/press-releases/wellnow-urgent-care-acquires-physicians-immediate-care/ (last accessed May 30, 2024).

[7] *Id.*

insurance information, dates of birth, financial account information, biometric data, and other sensitive information.

96. Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of the Notice from Defendants, dated February 22, 2024. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

Defendants' Failed Response to the Breach

97. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiffs' and Class Members' PHI/PII.

98. Not until roughly 10 months after Defendants claim to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PHI/PII Defendants confirmed were potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendants recommended next steps.

99. The Notice included, *inter alia*, the claim Defendants learned of the Data Breach on April 25, 2023.

100. Defendants had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law and their own assurances and representations to keep Representative Plaintiffs' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

101. Representative Plaintiffs and Class Members were required to provide their PHI/PII to Defendants in order to receive services, and as part of providing services, Defendants created, collected and stored Representative Plaintiffs' and Class Members' PHI/PII with the reasonable

expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

102. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

103. Representative Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' PHI/PII.

Defendants Collected/Stored Class Members' PHI/PII

104. Defendants acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII.

105. While providing healthcare services, Defendants receive, create and handle an incredible amount of Private PHI/PII including, *inter alia*, names, addresses, dates of birth, addresses, phone numbers, email addresses, Social Security numbers and medical information such as dates of service, diagnosis/treatment information, medical billing/claims information, health insurance information and other information that Defendants may deem necessary to provide services and care.

106. Patients are required to provide and to otherwise entrust their PHI/PII to Defendants to receive healthcare services and, in return, they reasonably and appropriately expect that Defendants will safeguard their highly sensitive PHI/PII and keep it secure and confidential.

107. The information held by Defendants in its computer systems included the unencrypted Private Information of Representative Plaintiffs and Class Members.

108. As a condition of their relationships with Representative Plaintiffs and Class Members, Defendants required that Representative Plaintiffs and Class Members entrust Defendants with highly sensitive and confidential PHI/PII. Defendants, in turn, stored that information on Defendants' system that was ultimately affected by the Data Breach.

109. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' PHI/PII, Defendants assumed legal and equitable duties over the PHI/PII and knew or should have known they were thereafter responsible for protecting Representative Plaintiffs' and Class Members' PHI/PII from unauthorized disclosure.

110. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiffs and Class Members relied on Defendants to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

111. Defendants could have prevented the Data Breach, which began no later than April 25, 2023, by properly securing and encrypting and/or more securely encrypting their servers generally, as well as Representative Plaintiffs' and Class Members' PHI/PII.

112. Defendants' negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

113. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendants were and/or certainly should have been on notice and aware of such attacks occurring in their industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants are large, sophisticated operations with the resources to put adequate data security protocols in place.

114. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

115. In failing to adequately secure Representative Plaintiffs' and Class Members' sensitive data, Defendants breached duties they owed Representative Plaintiffs and Class Members under statutory and common law.

116. Under HIPAA, health insurance providers have an affirmative duty to keep patients' PHI/PII confidential. As covered entities, Defendants have a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

117. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive PHI/PII to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their PHI/PII, independent of any statute.

118. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), they are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information") and Security Rule

("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

119. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

120. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

121. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

122. "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

123. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

124. HIPAA also requires Defendants to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic

protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

125. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

126. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

127. In addition to their obligations under federal and state laws, Defendants owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in Defendants' possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendants owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks and protocols adequately protected Representative Plaintiffs' and Class Members' PHI/PII.

128. Defendants owed a duty to Representative Plaintiffs and Class Members to design, maintain and test their computer systems, servers and networks to ensure that all PHI/PII in their possession was adequately secured and protected.

129. Defendants owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in their possession, including not sharing information with other entities who maintained substandard data security systems.

130. Defendants owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on their data security systems in a timely manner.

131. Defendants owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

132. Defendants owed a duty to Representative Plaintiffs and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust their PHI/PII to Defendants.

133. Defendants owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

134. Defendants owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

135. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete

record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

136. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[10]

137. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[11] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[12] In short, these sorts of data breaches are

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 30, 2024).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 30, 2024).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 30, 2024).

[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed May 30, 2024).

[12] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed May 30, 2024).

increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[13]

138. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

139. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

140. Identity thieves can use PHI/PII, such as that of Representative Plaintiffs and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[13] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed May 30, 2024).

141. The ramifications of Defendants' failure to keep secure Representative Plaintiffs' and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiffs' and Class Members' PHI/PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

142. There may be a time lag between when harm occurs versus when it is discovered and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

143. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[15]

144. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy

---

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf/ (last accessed May 30, 2024).

[15] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed May 30, 2024).

Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

145. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Representative Plaintiffs and Class Members.

146. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[18]

147. And data breaches are preventable.[19] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[20] She added that "[o]rganizations that collect, use, store, and share sensitive

---

16 *Id*.

17 *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed May 30, 2024).

18 *Id*.; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed May 30, 2024).

19 Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

20 *Id.* at 17.

personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[21]

148. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[22]

149. Here, Defendants knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendants knew or should have known that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Representative Plaintiffs and Class Members. Their failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

150. Defendants disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions, (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time,

[21] *Id.* at 28.

[22] *Id.*

and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

Representative Plaintiffs & Class Members Have Suffered Compensable Damages

151. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Representative Plaintiffs and Class Members significant injuries and harm in several ways.

152. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

153. In order to mitigate against the risks of identity theft and fraud, Representative Plaintiffs and members of the Class must immediately devote time, energy, and money to: (i) closely monitor their medical statements, bills, records, and credit and financial accounts; (ii) change login and password information on any sensitive account even more frequently than they already do; (iii) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (iv) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

154. Once PHI/PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason,

Representative Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct.

155. Furter, the value of Representative Plaintiffs' and Class Members' PHI/PII has been diminished by its exposure in the Data Breach.

156. Representative Plaintiffs and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

157. Representative Plaintiffs and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect its patients' PHI/PII.

158. Representative Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

159. Representative Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendants. Representative Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

160. Representative Plaintiffs and Class Members would not have obtained services from Defendants had they known that Defendants failed to properly train its employees, lacked

safety controls over its computer network, and did not have proper data security practices to safeguard their PHI/PII from criminal theft and misuse.

161. Finally, in addition to a remedy for the economic harm, Representative Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PHI/PII remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

162. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiffs and the following class (the "Class"):

> **Nationwide Class:** "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendants on April 25, 2023."

163. In addition, or in the alternative, Plaintiff Williams proposes the following Washington Class definition, subject to amendment as appropriate (together with the Nationwide Class, the "Class"):

> **Washington Class:** "All individuals within the state of Washington whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendants on April 25, 2023."

164. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors and any entity in which Defendants have a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards,

sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

165. In the alternative, Representative Plaintiffs request additional subclasses as necessary based on the types of PHI/PII that were compromised.

166. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

167. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. **Numerosity:** A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is sufficiently numerous. Membership in the Class will be determined by analysis of Defendants' records.

b. **Commonality:** Representative Plaintiffs and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendants had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

3) Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendants adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their PHI/PII had been compromised;

7) How and when Defendants actually learned of the Data Breach;

8) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiffs' and Class Members' PHI/PII;

9) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendants engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct; and

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

c. **Typicality:** Representative Plaintiffs' claims are typical of the claims of the Plaintiff Class. Representative Plaintiffs and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. **Adequacy of Representation:** Representative Plaintiffs in this class action are adequate representatives of the Plaintiff Class in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. **Superiority of Class Action:** Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

168. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

169. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

170. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PHI/PII of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

171. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

NEGLIGENCE
(On behalf of the Nationwide Class)

172. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

173. At all times herein relevant, Defendants owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' PHI/PII on their computer systems and networks.

174. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in their possession;

b. to protect Representative Plaintiffs' and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

175. Defendants knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

176. Defendants knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

177. Defendants knew or should have known that their data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII.

178. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiffs and Class Members had entrusted to them.

179. Defendants breached their duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

180. Because Defendants knew that a breach of their systems could damage numerous individuals, including Representative Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PHI/PII contained thereon.

181. Representative Plaintiffs' and Class Members' willingness to entrust Defendants with their PHI/PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PHI/PII stored on them from attack. Thus, Defendants had a special relationship with Representative Plaintiffs and Class Members.

182. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Representative Plaintiffs' and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants and Representative Plaintiffs and/or the remaining Class Members.

183. Defendants breached their general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiffs' and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train their employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

184. Defendants' willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

185. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

186. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

187. Defendants breached their duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting roughly ten months after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing

to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continue to breach their disclosure obligations to Representative Plaintiffs and Class Members.

188. Further, through their failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendants prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their PHI/PII.

189. There is a close causal connection between Defendants' failure to implement security measures to protect Representative Plaintiffs' and Class Members' PHI/PII and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PHI/PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

190. Defendants' wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

191. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

192. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect

PHI/PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

193. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

194. Defendants' violation of 15 U.S.C. § 45 constitutes negligence *per se.* Defendants also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

195. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII

compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

196. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

197. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII in their continued possession.

SECOND CLAIM FOR RELIEF

BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class)

198. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

199. Breach of implied contract is pled in the alternative to unjust enrichment.

200. Through their course of conduct, Defendants, Representative Plaintiffs and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PHI/PII.

201. Defendants required Representative Plaintiffs and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendants' services from Defendants.

202. Defendants solicited and invited Representative Plaintiffs and Class Members to provide their PHI/PII as part of Defendants' regular business practices. Representative Plaintiffs and Class Members accepted Defendants' offers and provided their PHI/PII to Defendants.

203. As a condition of being direct customers and/or employees of Defendants, Representative Plaintiffs and Class Members provided and entrusted their PHI/PII to Defendants. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if their data had been breached and compromised or stolen.

204. Implicit in the agreement between Representative Plaintiffs and Class Members and Defend, was Defendant's obligation to: (a) use such PII and PHI for business purposes only; (b) take reasonable steps to safeguard Plaintiffs' and Class Members' PII and PHI; (c) prevent unauthorized access and/or disclosure of Plaintiffs' and Class Members' PII and PHI; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiffs and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiffs' and Class Members' PII and PHI under conditions that kept such information secure and confidential.

205. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their PHI/PII to Defendants, in exchange for, amongst other things, the protection of their PHI/PII.

206. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

207. Defendants breached the implied contracts they made with Representative Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

208. As a direct and proximate result of Defendants' above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH & FAIR DEALING
(On behalf of the Nationwide Class)

209. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

210. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

211. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendants.

212. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class

Members and continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

213. Defendants acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing injury in an amount to be determined at trial.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT
(On behalf of the Nationwide Class)

214. Unjust enrichment is pled in the alternative to Representative Plaintiffs' and Class Members' common law causes of action.

215. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Representative Plaintiffs and Class Members.

216. Defendants, prior to and at the time Representative Plaintiffs and Class Members entrusted their PHI/PII to Defendants for the purpose of purchasing services from Defendants, caused Representative Plaintiffs and Class Members to reasonably believe that Defendants would keep such PHI/PII secure.

217. Defendants were aware, or should have been aware, that reasonable consumers would have wanted their PHI/PII kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were substandard for that purpose.

218. Defendants were also aware that if the substandard condition of and vulnerabilities in their information systems were disclosed, they would have negatively affected Representative Plaintiffs' and Class Members' decisions to engage with Defendants.

219. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Representative Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Representative Plaintiffs and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Representative Plaintiffs and Class Members.

220. Defendants were unjustly enriched at the expense of Representative Plaintiffs and Class Members. Defendants received profits, benefits and compensation, in part, at the expense of Representative Plaintiffs and Class Members. By contrast, Representative Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

221. Since Defendants' profits, benefits and other compensation were obtained by improper means, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits they realized from these transactions.

222. Representative Plaintiffs and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiffs and Class Members may seek restitution.

FIFTH CAUSE OF ACTION

VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code Ann. §§19.86.020, *et seq.*
(*On behalf of Plaintiff Williams & the Washington Class*)

223. Plaintiff Williams re-alleges and incorporates the foregoing allegations above as if fully set forth herein.

224. Defendants are a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

225. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

226. Defendants engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a) Failing to secure and protect Plaintiff Williams' and Washington Class Members' PHI/PII in a confidential manner;

b) Failing to inform Plaintiff Williams and Washington Class Members of the extent of Defendants' data collection, storage, and disclosure practices;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Williams and Washington Class members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the unauthorized disclosure of their PHI/PII;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Williams and Washington Class members' PHI/PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Williams and Washington Class members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

f) Misrepresenting that certain sensitive PHI/PII would not be disclosed to third parties;

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Williams' and Washington Class Members' PHI/PII; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security

> and privacy of Plaintiff Williams' and Washington Class members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

227. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' ability and intentions to protect the confidential and sensitive PHI/PII of Plaintiff Williams and Washington Class Members communicated for the purpose of medical treatment.

228. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Williams and the Washington Class Members, that their PHI/PII would be held in a secure and confidential manner, rather than deliberately disclosed to third parties.

229. Defendants acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff Williams' and Washington Class Members' rights.

230. Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010*, et seq.*.

231. Alternatively, Defendants' conduct is injurious to the public interest because it has injured Plaintiff Williams and Washington Class Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washington Residents impacted by Defendants' failure to secure Plaintiff Williams' and Class Member's PHI/PII.

232. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiff Williams and Washington Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary

and non-monetary damages, including the damage to their privacy and property interests in their PHI/PII.

233. Plaintiff Williams and Washington Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

SIXTH CAUSE OF ACTION

VIOLATION OF THE WASHINGTON HEALTH CARE INFORMATION ACT
RCW 70.2.005, *et seq.*
(*On behalf of Plaintiff Williams & the Washington Class*)

234. Plaintiff Williams re-alleges and incorporates the foregoing allegations above as if fully set forth herein.

235. The Washington HCIA, RCW 70.2.005, et seq., states that "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization."

236. The HCIA defines "health care information" to mean "any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care …." RCW 70.02.010(17).

237. Defendants are a health care facility as defined by RCW 70.010(16).

238. By capturing its patients' personally identifiable and health information and failing to protect it from disclosure to unauthorized third parties, Defendants disclosed Plaintiff Williams' and Washington Class members' health care information without their written authorization.

239. As a direct and proximate cause of Defendants' actions, Plaintiff Williams and Washington Class members were damaged in that:

a) Sensitive, confidential, and/or protected information that Plaintiff and Washington Class members intended to remain private is no more;

b) Defendants took something of value from Plaintiff and Washington Class members and derived benefit therefrom without Plaintiff's and Washington Class members' knowledge or informed consent and without sharing the benefit of such value;

c) Plaintiff and Washington Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality of patient data and communications and

d) Defendant's actions diminished the value of Plaintiff's and Washington Class members' personally identifiable patient data and communications.

240. Plaintiff Williams and Washington Class members seek an order requiring Defendants to comply with the HCIA, actual damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Representative Plaintiffs, Genevieve Tambroni, John Lattimore, (as parent for minor children S.L. and V.L), Ella Williams, James Beach, Caitlin McDaniel, Claudine King, and Ian Curro individually and on behalf of all others similarly situated, respectfully request this Honorable Court to enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and/or any other appropriate subclasses under Federal Rules of Civil Procedure Rules 23(b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

c. requiring Defendants to delete and purge Representative Plaintiffs' and Class Members' PHI/PII unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PHI/PII;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendants' systems on a periodic basis;

f. prohibiting Defendants from maintaining Representative Plaintiffs' and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiffs and Class Members;

j. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personally identifiable information;

k. requiring Defendants to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifiable information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of the Plaintiff Class, hereby demand a trial by jury for all issues triable by jury.

Dated: June 7, 2024,

Respectfully Submitted,

By: */s/ David S. Almeida*

David S. Almeida (ARDC 6285557)
Britany A. Kabakov (ARDC 6336126)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614

Telephone: (312) 576-3024
Email: david@almeidalawgroup.com
Email: britany@almeidalawgroup.com

Laura Van Note, Esq. (CA S.B. #310160)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Email: lvn@colevannote.com

Brandon M. Wise, Esq. (IL S.B. Bar # 6319580)
Andrew R. Tate, Esq. (GA Bar #518068)*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Telephone: 314-833-4825
Email: bwise@peifferwolf.com
Atate@peifferwolf.com

Daniel Srourian, Esq. (SBN 285678) *
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: 213.474.3800
Email: daniel@slfla.com

Kevin Laukaitis, Esq.*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462
Email:klaukaitis@laukaitislaw.com

**Pro hac vice anticipated*

Attorneys for Representative Plaintiffs & the Proposed Class

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this date, a true and accurate copy of the foregoing document was filed with the Clerk of the Court using the CM/ECF efiling system, which will provide notice and allow access to all counsel of record.

/s/ David S. Almeida